ASA 8.3 Issue: MSS Exceeded - HTTP Clients Cannot Browse to Some Websites

Contents

Introduction

This document describes an issue that occurs when some websites are not accessible through an Adaptive Security Appliance (ASA) that runs version 8.3 or later software.

The ASA 7.0 release introduces several new security enhancements, one of which is a check for TCP endpoints which adhere to the advertised Maximum Segment Size (MSS). In a normal TCP session, the client sends a SYN packet to the server, with the MSS included within the TCP options of the SYN packet. The server, upon receipt of the SYN packet, should recognize the MSS value sent by the client and then send its own MSS value in the SYN-ACK packet. Once both the client and the server are aware of each other's MSS, neither peer should send a packet to the other that is greater than that peer's MSS.

A discovery has been made that there are a few HTTP servers on the Internet that do not honor the MSS that the client advertises. Subsequently, the HTTP server sends data packets to the client that are larger than the advertised MSS. Before release 7.0, these packets were allowed through the ASA. With the security enhancement included in the 7.0 software release, these packets are dropped by default. This document is designed to assist the Cisco Adaptive Security Appliance administrator in the diagnosis of this problem and the implementation of a workaround to allow the packets that exceed the MSS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on a Cisco Adaptive Security Appliance (ASA) that runs version 8.3 software.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This section presents you with the information to configure the features this document describes.

Network Diagram

This document uses this network setup:

ASA 8.3 Configuration

These configuration commands are added to an ASA 8.3 default configuration in order to allow the HTTP client to communicate with the HTTP server.

ASA 8.3 Configuration

```
ASA(config)#interface Ethernet0
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 192.168.9.30 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface Ethernet1
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 10.0.0.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#object network Inside-Network
ASA(config-obj)#subnet 10.0.0.0 255.0.0.0
ASA(config)#nat (inside,outside) source dynamic Inside-Network interface
ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.2 1
```

Troubleshoot

If a particular website is not accessible through the ASA, complete these steps to troubleshoot. You first need to capture the packets from the HTTP connection. In order to collect the packets, the relevant IP addresses of the HTTP server and client need to be known, as well as the IP address that the client is translated to when it traverses the ASA.

In the example network, the HTTP server is addressed at 192.168.9.2, the HTTP client is addressed at 10.0.0.2, and the HTTP client addresses is translated to 192.168.9.30 as packets leave the outside interface. You can use the capture feature of the Cisco Adaptive Security Appliance (ASA) in order to collect the packets, or you can utilize an external packet capture. If you intend to use the capture feature, the administrator can also utilize a new capture feature

included in the 7.0 release that allows the administrator to capture packets that are dropped due to a TCP anomaly.

Note: Some of the commands in these tables wrap to a second line due to spatial restrictions.

1. Define a pair of access lists that identify the packets as they ingress and egress the outside and inside interfaces.
2. Enable the capture feature for both the inside and outside interface. Also enable the capture for TCP-specific MSS-exceeded packets.
3. Clear the Accelerated Security Path (ASP) counters on the ASA.
4. Enable trap syslogging at the debug level sent to a host on the network.
5. Initiate an HTTP session from the HTTP client to the problematic HTTP server, and collect the syslog output and the output from these commands after the connection fails.**show capture capture-insideshow capture capture-outsideshow capture mss-captureshow asp dropNote:** Refer to System Log Message 419001 for more information about this error message.

Workaround

Implement a workaround now that you know that the ASA drops the packets that exceed the MSS value advertised by the client. Keep in mind that you might not want to allow these packets to reach the client because of a potential buffer overrun on the client. If you choose to allow these packets through the ASA, proceed with this workaround procedure.

Modular Policy Framework (MPF) is a new feature in the 7.0 release that is used to allow these packets through the ASA. This document is not designed to fully detail the MPF but rather suggests the configuration entities used to work around the problem. Refer to the ASA 8.3 Configuration Guide for more information on MPF.

An overview to the workaround includes the identification of the HTTP client and servers via an access list. Once the access list is defined, a class map is created and the access list is assigned to the class map. Then a TCP map is configured and the option to allow packets that exceed the MSS is enabled. Once the TCP map and class map are defined, you can add them to a new or an existing policy map. A policy map is then assigned to a security policy. Use the **service-policy** command in configuration mode to activate a policy map globally or on an interface. These configuration parameters are added to the Cisco Adaptive Security Appliance (ASA) 8.3 Configuration List. After you create a policy map named "http-map1," this sample configuration adds the class map to this policy map.

Specific Interface: MPF Configuration to Allow Packets that Exceed MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match access-list http-list2
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
```

```
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 interface outside
ASA#
```

Once these configuration parameters are in place, packets from 192.168.9.2 that exceed the MSS advertised by the client are allowed through the ASA. It is important to note that the access list used in the class map is designed to identify outbound traffic to 192.168.9.2. The outbound traffic is examined to allow the inspection engine to extract the MSS from the outgoing SYN packet. Therefore, it is imperative to configure the access list with the direction of the SYN in mind. If a more pervasive rule is required, you can replace the **access-list** statement in this section with an **access-list** statement that permits everything, such as **access-list http-list2 permit ip any any** or **access-list http-list2 permit tcp any any**. Also remember that the VPN tunnel can be slow if a large value of TCP MSS is used. You can reduce TCP MSS to improve the performance.

This example helps to configure globally inbound and outbound traffic in the ASA:

Global Configuration: MPF Configuration to Allow Packets that Exceed MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match any
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 global
ASA#
```

Verify

This section provides information you can use to confirm your configuration works properly.

Repeat the steps in the Troubleshoot section in order to verify that the configuration changes do what they are designed to do.

Syslogs from a Successful Connection

```
%ASA-6-609001: Built local-host inside:10.0.0.2
%ASA-6-609001: Built local-host outside:192.168.9.2
%ASA-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58798
               to outside:192.168.9.30/1025
%ASA-6-302013: Built outbound TCP connection 13 for outside:192.168.9.2/80
               (192.168.9.2/80) to inside:10.0.0.2/58798 (192.168.9.30/1025)
%ASA-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

%ASA-6-302014: Teardown TCP connection 13 for outside:192.168.9.2/80 to
               inside:10.0.0.2/58798 duration 0:00:01 bytes 6938 TCP FINs
```

!--- The connection is built and immediately !--- torn down when the web content is retrieved.

Output from show Commands from a Successful Connection

```
ASA#
ASA#show capture capture-inside
21 packets captured
   1: 09:16:50.972392 10.0.0.2.58769 > 192.168.9.2.80: S
      751781751:751781751(0)
   win 1840 <mss 460,sackOK,timestamp 110313116 0,nop,wscale 0>

 !--- The advertised MSS of the client is 460 in packet #1. However, !--- with th workaround in place,
packets 7, 9, 11, 13, and 15 appear !--- on the inside trace, despite the MSS>460. 2: 09:16:51.098536
192.168.9.2.80 > 10.0.0.2.58769: S 1305880751:1305880751(0) ack 751781752 win 8192 <mss 1380> 3:
09:16:51.098734 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305880752 win 1840 4: 09:16:51.099009 10.0.0.2.
> 192.168.9.2.80: P 751781752:751781851(99) ack 1305880752 win 1840 5: 09:16:51.228412 192.168.9.2.80 >
10.0.0.2.58769: . ack 751781851 win 8192 6: 09:16:51.228641 192.168.9.2.80 > 10.0.0.2.58769: . ack 7517
win 25840 7: 09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: . 1305880752:1305882112(1360) ack 7517818
25840
   8: 09:16:51.237704 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305882112 win 4080
   9: 09:16:51.243593 192.168.9.2.80 > 10.0.0.2.58769: P
      1305882112:1305883472(1360) ack 751781851 win 25840
  10: 09:16:51.243990 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305883472 win 6800
  11: 09:16:51.251009 192.168.9.2.80 > 10.0.0.2.58769: .
      1305883472:1305884832(1360) ack 751781851 win 25840
  12: 09:16:51.252428 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305884832 win 9520
  13: 09:16:51.258440 192.168.9.2.80 > 10.0.0.2.58769: P
      1305884832:1305886192(1360) ack 751781851 win 25840
  14: 09:16:51.258806 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305886192 win 12240
  15: 09:16:51.266130 192.168.9.2.80 > 10.0.0.2.58769: .
      1305886192:1305887552(1360) ack 751781851 win 25840
  16: 09:16:51.266145 192.168.9.2.80 > 10.0.0.2.58769: P
      1305887552:1305887593(41) ack 751781851 win 25840
  17: 09:16:51.266511 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887552 win 14960
  18: 09:16:51.266542 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887593 win 14960
  19: 09:16:51.267320 10.0.0.2.58769 > 192.168.9.2.80: F
      751781851:751781851(0) ack 1305887593 win 14960
  20: 09:16:51.411370 192.168.9.2.80 > 10.0.0.2.58769: F
      1305887593:1305887593(0) ack 751781852 win 8192
  21: 09:16:51.411554 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887594 win 14960
21 packets shown
ASA#
ASA#
ASA#show capture capture-outside
21 packets captured
   1: 09:16:50.972834 192.168.9.30.1024 > 192.168.9.2.80: S
      1465558595:1465558595(0) win 1840 <mss 460,sackOK,timestamp
      110313116 0,nop,wscale 0>
   2: 09:16:51.098505 192.168.9.2.80 > 192.168.9.30.1024:
      S 466908058:466908058(0) ack 1465558596 win 8192 <mss 1460>
   3: 09:16:51.098749 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466908059 win 1840
   4: 09:16:51.099070 192.168.9.30.1024 > 192.168.9.2.80: P
      1465558596:1465558695(99) ack 466908059 win 1840
   5: 09:16:51.228397 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 8192
   6: 09:16:51.228625 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 25840
```

```
   7: 09:16:51.236224 192.168.9.2.80 > 192.168.9.30.1024: .
      466908059:466909419(1360 ack 1465558695 win 25840
   8: 09:16:51.237719 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466909419 win 4080
   9: 09:16:51.243578 192.168.9.2.80 > 192.168.9.30.1024: P
      466909419:466910779(1360) ack 1465558695 win 25840
  10: 09:16:51.244005 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466910779 win 6800
  11: 09:16:51.250978 192.168.9.2.80 > 192.168.9.30.1024: .
      466910779:466912139(1360) ack 1465558695 win 25840
  12: 09:16:51.252443 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466912139 win 9520
  13: 09:16:51.258424 192.168.9.2.80 > 192.168.9.30.1024: P
      466912139:466913499(1360) ack 1465558695 win 25840
  14: 09:16:51.258485 192.168.9.2.80 > 192.168.9.30.1024: P
      466914859:466914900(41) ack 1465558695 win 25840
  15: 09:16:51.258821 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466913499 win 12240
  16: 09:16:51.266099 192.168.9.2.80 > 192.168.9.30.1024: .
      466913499:466914859(1360) ack 1465558695 win 25840
  17: 09:16:51.266526 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914859 win 14960
  18: 09:16:51.266557 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914900 win 14960
  19: 09:16:51.267335 192.168.9.30.1024 > 192.168.9.2.80: F
      1465558695:1465558695(0) ack 466914900 win 14960
  20: 09:16:51.411340 192.168.9.2.80 > 192.168.9.30.1024: F
      466914900:466914900(0) ack 1465558696 win 8192
  21: 09:16:51.411569 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914901 win 14960
21 packets shown
ASA#
ASA(config)#show capture mss-capture
0 packets captured
0 packets shown
ASA#
ASA#show asp drop

Frame drop:

Flow drop:
ASA#

!--- Both the show capture mss-capture and the show asp drop
!--- commands reveal that no packets are dropped.
```

Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances]
- [Security Product Field Notices (including Cisco Adaptive Security Appliance (ASA))]
- [Requests for Comments (RFCs)]
- [Technical Support & Documentation - Cisco Systems]